Tampereen yliopisto

Tuomas Kauppinen

KÄYTTÄJÄTIETOJEN VARJELU

Vaatimukset ja menetelmät

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Syyskuu 2019

TIIVISTELMÄ

Tuomas Kauppinen: Käyttäjätietojen varjelu – Vaatimukset ja menetelmät
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Syyskuu 2019

Tutkielma tarkastelee miten Euroopan unioni velvoittaa yrityksiä, jotka käsittelevät EU:n kansalaisten henkilötietoja ja miten uusi tietoturva-asetus vaikutti asiaan. Käsitellään mitä uhkia yritykset kohtaavat suojellessaan asiakastietojaan ja järjestelmiään, ja miten niitä torjutaan. Sekä ohjeistetaan käyttäjien keinoja maksimoida tietojensa turvallisuus. Tutkielmassa käydään myös läpi käyttäjätietojen yksityisyyden vaarantavia tekijöitä, kuten tietomurrot, ja esitellään ratkaisuja niiden ennaltaehkäisemiseksi, ja keinoja jo tapahtuneista onnettomuuksista toipumiseksi. Tämä tutkielma on kirjallisuuskatsaus, joten tieto perustuu pääosin alan olemassa olevaan kirjallisuuteen.

Avainsanat: Käyttäjätiedot, Yksityisyys, Tietoturvallisuus, Tietomurto, GDPR

Sisällys

1 Johdanto

Yhteiskunnan jatkuva digitalisoituminen ja sosiaalisen median aikakausi on tuottanut valtavan määrän digitaalista informaatiota käyttäjistään. Käyttäjät ovat jakaneet kiihtyvällä tahdilla dataa itsestään, paljastaen osia yksityiselämästään sosiaalisen median kanavissa. Tietoyhteiskunnan kasvaessa myös henkilötietoihin tunkeutuminen on lisääntynyt. [Aïmeur and Lafond 2013.] Ihmisten huolenaiheeksi on noussut henkilötietojen turvallisuus, lehtien uutisoidessa massiivisista tietomurroista maailmanlaajuisesti tunnetuissa yrityksissä. Mutta miten eri tahot voivat vaikuttaa käyttäjätietojen suojeluun? Pyrin selvittämään millä tavoin eri osapuolet vaikuttavat omalta osaltaan käyttäjätietojen varjeluun ja miten omia tietojaan voi suojella paremmin, tuoden ilmi uhkia ja keinoja kyseisten uhkien ennakoimiseen ja välttämiseen.

Tutkielman lähteet ovat peräisin Tampereen yliopiston tarjoamista elektronisista aineistoista ja muualta verkosta. Lähteitä valittaessa on arvioitu niiden luotettavuutta ja todenmukaisuutta. Aineistojen tarjonnasta on valittu kirjallisuutta, joka vastasi parhaiten työn aihetta. Valinnassa pyrittiin keskittymään julkisen sektorin toimintaan ja välttämään yksittäisiä, esimerkiksi pelkästään terveydenhoitoalalla ilmeneviä, henkilötietojen varjeluongelmia ja ainoastaan niihin soveltuvia sovellusratkaisuja, koska niiden määrä on liian massiivinen tutkielman laajuuteen verrattuna.

Ensin tutkielmassa tutustutaan, miten EU:n määräämä uusi tietosuoja-asetus vaikutti henkilötietojen käsittelyyn. Sitten käsitellään mitä tietomurrot ovat, ja mistä ne yleisimmin aiheutuvat. Käydään läpi keinoja, joilla yritykset voivat turvata järjestelmänsä ja käsittelemänsä informaation. Selvitetään miten viimevuosina yleistynyt kaksivaiheinen tunnistautuminen parantaa henkilötietojen ja järjestelmien turvallisuutta. Sekä lopuksi esitellään miten tavalliset käyttäjät voivat vaikuttaa käyttäjätiliensä turvallisuuteen.

2 Miten EU vaikuttaa käyttäjätietojen suojeluun

Tässä luvussa tarkastellaan miten EU-maissa 2018 voimaan astunut yleinen tietosuoja-asetus vaikutti yritysten asiakastietojen käsittelyyn. Käydään läpi vanhan tietosuojadirektiivin ja uuden asetuksen pääkohtia ja eroavaisuuksia, siirtymisprosessia ja asetuksesta seuranneita rangaistuksia.

2.1 Vanha tietosuojadirektiivi

Vuodesta 1995 asti voimassa ollut *DPD* (Data Protection Directive), tunnettiin suomessa nimillä henkilötietodirektiivi ja tietosuojadirektiivi. Direktiivi on kuitenkin vain kansalliselle lainsäätäjälle suunnattu toimintaohje, jota tässä tapauksessa valvoi Suomen tietosuojavaltuutettu, kun taas 2018 voimaan astunut asetus on itsessään suoraan yrityksiä velvoittava. [Valtiovarainministeriö 2016.]

Direktiivin voimassaoloaikana tapahtui valtavasti kehitystä digitaalisella saralla. Kyseisen 20 vuoden aikana direktiivin määrittely ja valvominen jäivät jälkeen ajastaan. Nykyinen sosiaalisten medioiden valtakausi ja digitalisoituminen on synnyttänyt valtavan määrän digitaalista informaatiota käyttäjistä, joten oli selkeästi tarvetta päivittää käyttäjien tietosuoja tälle vuosituhannelle.

2.2 Yleinen tietosuoja-asetus

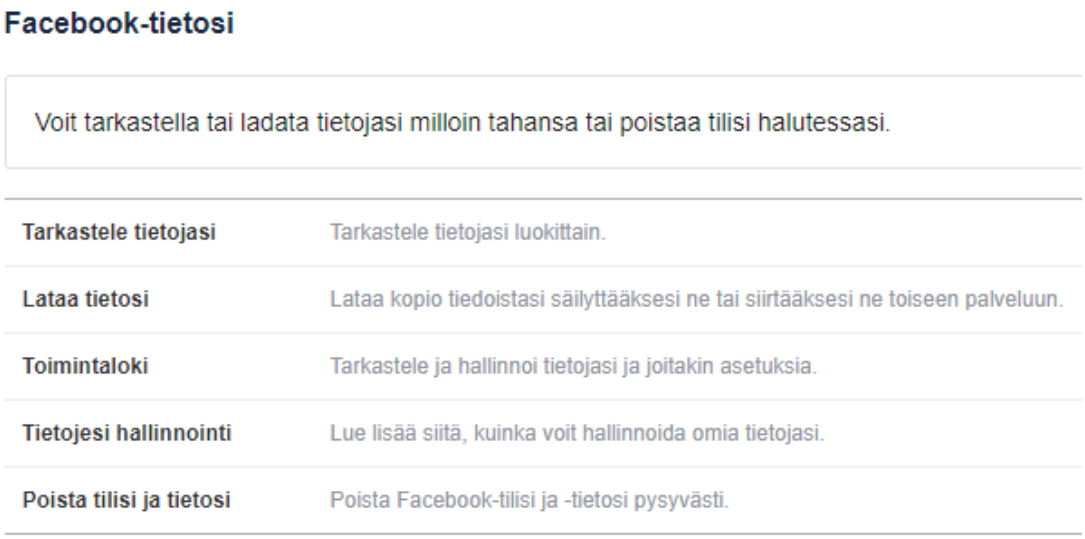
GDPR lyhenne muodostuu sanoista General Data Protection Regulation, ja se tunnetaan suomessa nimellä yleinen tietosuoja-asetus. Se on uusi henkilötietojen käsittelyä sääntelevä laki, jota on sovellettu kaikissa EU-maissa 25.5.2018 alkaen [Tietosuojavaltuutetun toimisto 2019]. Laki koskee kaikkien EU-maissa asuvien kansalaisten henkilötietoja, huolimatta yrityksen sijainnista [Meszaros 2018]. Yleisen tietosuoja-asetuksen tarkoitus on parantaa henkilötietojen suojaa ja tietosuojaoikeuksia, vastata nykyaikaisiin tietosuojakysymyksiin, yhtenäistää tietosuojasääntelyä EU-maissa sekä edistää digitaalisten sisämarkkinoiden kehitystä [Tietosuojavaltuutetun toimisto 2019].

Käyttäjillä on GDPR:n myötä selkeästi paremmat oikeudet omia tietojaan koskien. Käyttäjällä on oikeus [Tietosuojavaltuutetun toimisto 2019]:

- tietää mitä henkilötietoja organisaatiolla on hänestä.
- tietää miten ja mihin tarkoitukseen hänen henkilötietojaan käsitellään.
- pyytää virheellisten, epätarkkojen ja puutteellisten henkilötietojensa korjaamista.
- pyytää henkilötietojensa poistamista.
- vastustaa henkilötietojensa käsittelyä.
- pyytää henkilötietojensa käsittelyn rajoittamista.
- siirtää tietonsa toiselle organisaatiolle
- olla joutumatta perusteetta automaattisen päätöksenteon kohteeksi.

- Saada ilmoitus tapahtuneesta tietomurrosta 72 tunnin sisällä [Meszaros 2018].

Kuvasta 1 käy ilmi, mitä vaihtoehtoja tietosuoja-asetusta noudattavan Facebook-yhteisöpalvelun käyttäjätietojen hallinta tarjoaa käyttäjilleen.



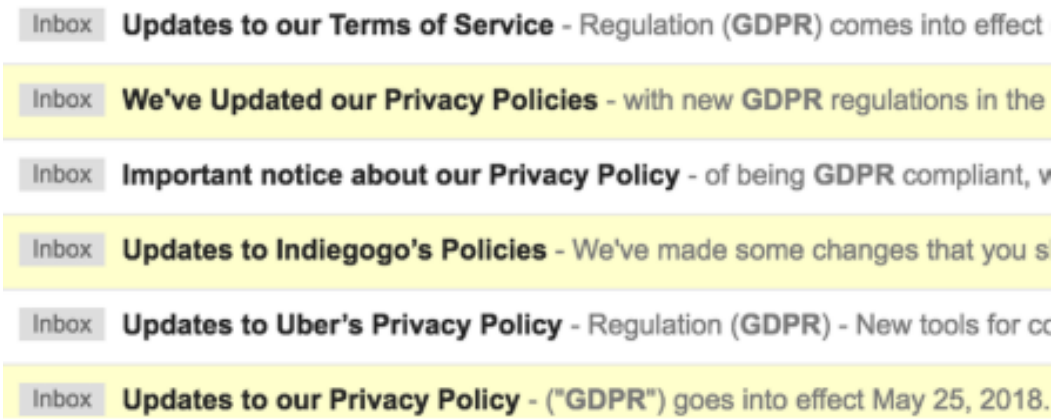
Kuva 1. Facebookin GDPR:n mukainen käyttäjätietojen hallinta. [Facebook 2019]

2.3 Direktiivin ja asetuksen eroavaisuudet

Vanhalla tietosuojadirektiivillä ja uudella yleisellä tietosuoja-asetuksella on paljon yhtäläisyyksiä. DPD sisälsi paljon hyvin samantyylisiä kohtia kuin GDPR, kuten asianomaiselle täytyy kertoa, jos hänen tietojaan kerätään, tietojen pitää olla turvassa mahdollisilta väärinkäytöksiltä ja asianomaisella täytyy olla oikeus tarkastella tietojaan ja korjata virheellisiä tietoja. Suurimpana erona on, että tietosuoja-asetus koskee myös EU:n ulkopuolella sijaitsevia yrityksiä, jos he tallentavat EU:n kansalaisten tietoja.

Vaikka tietosuojadirektiivin ja yleisen tietosuoja-asetuksen sisällöt ovat lähellä toisiaan, asetuksen voimaan astuminen näkyi selkeästi yritysten toiminnassa. Asiakkaiden sähköpostit täyttyivät päivitettyjen yksityisyyskäytäntöjen ilmoituksista (Kuva 2). Ja nykyään

täytyy lähes poikkeuksetta hyväksyä yritysten verkkosivujen käyttöehdot ja evästeiden käyttö sivustolle saavuttaessa.



Kuva 2. Tietosuojakäytäntöjen päivitysilmoitukset täyttivät asiakkaiden sähköpostit GDPR:n astuessa voimaan. [Business Insider 2018]

2.4 GDPR:n rikkomisesta seuraavat rangaistukset

Yritysten suurimpana motivaattorina toimii rangaistuksen pelko. GDPR:n rikkomisesta voi saada sakkoa jopa 20 miljoonaa euroa tai 4 prosenttia yrityksen vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta, sakoksi määräytyy suurempi kyseisistä summista [eugdpr.org 2019]. Esimerkiksi Britanniassa GDPR:n toteuttamista valvova taho *ICO* (Information Commissioner's Office) on määrännyt British Airways -yhtiölle 183 miljoonan punnan sakot vuonna 2019, noin 500 000 asiakkaan henkilötietojen vuotamisesta. Vuodettujen tietojen joukossa oli muun muassa nimiä, osoitteita ja luottokorttitietoja, sisältäen luottokorttien numeroita, voimassaolopäivämääriä sekä CVC-koodeja. Tietoja oltaisiin voitu käyttää korttipetosten ja jopa identiteettivarkauksien suorittamiseen, joten määrätyt sakot ovat täysin aiheelliset. [Macaulay 2019.]

Britannian ICO määräsi sakkoja myös Marriott-hotelliketjulle. Ketjun tietomurrossa vuoti jopa 500 miljoonan asiakkaan tietoja. Vuodetut tiedot sisälsivät muun muassa maksutietoja, sähköpostiosoitteita, puhelinnumeroita ja passien numeroita. Tietomurto alkoi jo vuonna 2014 ja paljastui vasta 2018 vuoden marraskuussa. Sakkoa Hotelliketju joutuu maksamaan 99 miljoonaa puntaa. [O'Flaherty 2019.]

Myös hakukonejätti Google on joutunut sakotettujen listalle. Google ei tarjonnut asiakkailleen tarpeeksi tietoa heidän henkilötietojensa keräämisestä eikä tapoja hallita heitä koskevan informaation käyttöä. Määrätyn sakon suuruus on 50 miljoonaa euroa, joka on vain murto-osa yhtiön vuosituotoista, vuoden 2018 viimeisellä vuosineljänneksellä yhtiö tuotti yli 30 miljardia dollaria. [Porter 2019.]

2.5 GDPR ja tutkimustyö

Tietosuoja-asetuksessa on otettu myös huomioon sen mahdollinen tutkimustyön rajoittaminen ja vaikeuttaminen. On määritetty tiettyjä vapautuksia, joilla mahdollistetaan tilastollisen ja tieteellisen tutkimuksen jatkuminen asetuksesta huolimatta, ja jotka ovat tärkeä askel kohti henkilötietojen keräämistä ja käyttöä tieteellisessä tutkimuksessa. [Meszaros 2018.] Esimerkiksi *kohta 33* (Recital 33) [Privazyplan 2019]:

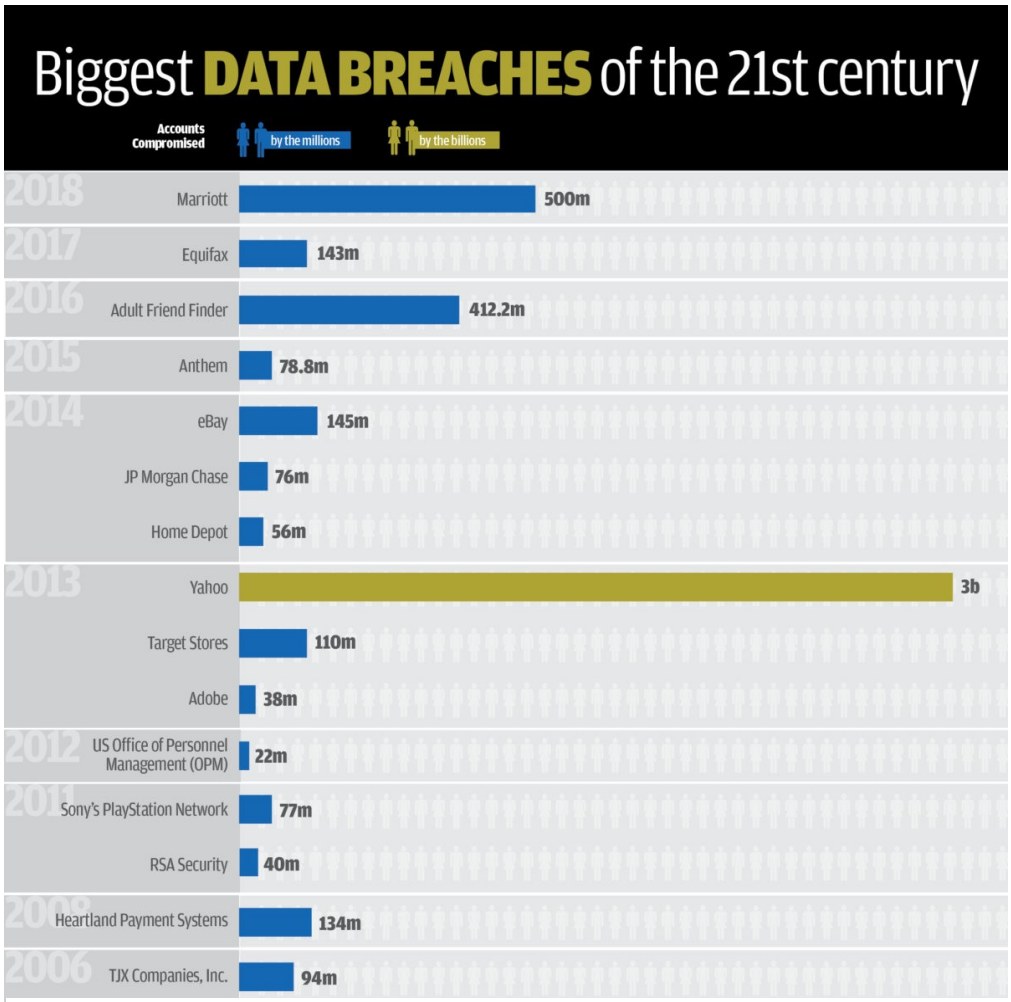
> ”Usein tieteellisiä tutkimustarkoituksia varten tehtävän käsittelyn tarkoitusta ei ole mahdollista täysin määrittää siinä vaiheessa, kun henkilötietoja kerätään. Tästä syystä rekisteröityjen olisi voitava antaa suostumuksensa tietyille tieteellisen tutkimuksen aloille silloin, kun noudatetaan tieteellisen tutkimuksen tunnustettuja eettisiä standardeja. Rekisteröidyillä olisi oltava mahdollisuus antaa suostumuksensa ainoastaan tietyille tutkimusaloille tai tutkimushankkeiden osille siinä määrin kuin tarkoitus sen mahdollistaa.”

3 Tietomurrot

3.1 Yleistietoa tietomurroista

Tietomurroksi kutsutaan tapausta, kun ulkopuolisella on luvaton pääsy arkaluontoisiin, suojattuihin tai luottamuksellisiin tietoihin. Tietovuoto tarkoittaa salassa pidettävän tiedon vuotoa ulkopuolisille [Suomisanakirja 2019]. Murron tapauksessa tietoa havitellaan jonkinasteisen hyökkäyksen muodossa, kun taas vuoto voi seurata inhimillisestä virheestä. Tutkielmassa keskitytään pääosin tietomurtoihin, joista puhuttaessa välillä sivutaan myös vahingoista johtuvia tietovuotoja.

Hakkerit voivat käyttää haltuunsa saamia tietojaan itse ja myydä niitä eteenpäin [Zou 2016]. Tietomurrot ovat yleistyneet niin yksityisellä, kuin julkisellakin sektorilla 2000-luvun aikana. Viime vuosina tietomurtojen uhriksi ovat joutuneet muun muassa Adobe, eBay, Target, Yahoo, Sony, Google ja Facebook, miljardien asiakkaiden tiedot ovat joutuneet vääriin käsiin. Kuva 3 sisältää 2000-luvun suurimpia tietomurtoja vaarantuneiden käyttäjätilien määrän mukaan.



Kuva 3. 2000-luvun suurimmat tietomurrot vaarantuneiden käyttäjätilien määrän mukaan [Armerding 2018].

Tietomurroilla on kaksi pääuhria: yritys tai järjestö ja sen asiakkaat, julkisen sektorin tapauksissa yksittäiset kansalaiset. Riippuen vuodetuista tiedoista, asiakkaat saattavat joutua tekemään toimenpiteitä, kuten kuolettamaan ja hankkimaan uusia maksuvälineitä. Tapahtuneen murron tullessa julkisuuteen yhtiön osakkeiden arvo voi pudota rajusti, tietoturvan laiminlyömisestä voi saada suuretkin sakot ja yrityksen imago saattaa kokea kovan kolauksen. Näistä syistä yritys saattaa pohtia tietomurrosta vaikenemista, mutta EU:n asukkaiden käyttäjätietoja koskevissa tapauksissa GDPR velvoittaa ilmoittamaan murrosta, ja Yhdysvalloissa ainakin 47 osavaltion lainsäädäntö vaatii tietomurtojen julkaisemisen. Yrityksillä on siis laillinen velvoite, sekä imagon suojelemiseksi on viisaampaa ilmoittaa murrosta itse, kuin jäädä jälkeenpäin kiinni asian piilottelusta. Tietomurtojen havaitsemisessa saattaa mennä kuukausia tai jopa vuosia, koska prosessi voi olla rauhallinen ja pitkäkestoinen. [Joseph 2017.]

3.2 Yleisimmät tietomurtojen aiheuttajat

Hakkerit hyödyntävät huonosti ohjelmoituja ohjelmistosovelluksia, takaportteja ja heikosti suunniteltuja tai implementoituja verkkojärjestelmiä. Niihin jää heikkouksia joiden kautta hakkerit pääsevät helposti käsiksi yritysten tietoihin. Täten on tärkeää varmistaa ohjelmistojen ja laitteistojen laatu, sekä pitää ne päivitettyinä ajan tasalle. [Sutcliffe 2019.]

Suorien ja epäsuorien haittaohjelmien käyttö on kasvussa. Haittaohjelman tarkoitus on päästä kohdejärjestelmään ilman käyttäjän varsinaista suostumusta, ja avata hakkerille väylä väärinkäyttää järjestelmää ja mahdollisesti muita siihen yhteydessä olevia järjestelmiä. Haittaohjelmia levitetään tunnetusti kyseenalaisten tai toisten yritysten sivustojen kaltaisiksi naamioitujen verkkosivujen, ja epäilyttävien sähköpostien kautta, joiden alkuperästä ei ole varmuutta. [Sutcliffe 2019.]

Välillä hakkerien ei edes tarvitse suunnata hyökkäystä järjestelmää kohti. He harrastavat myös sosiaalista manipulointia, vakuuttelemalla ja huijaamalla he voivat saada henkilöltä tietoja ja pääsyn käsiksi tarvitsemaansa dataan. Esimerkiksi sähköpostihuijaukset ovat sosiaalista manipulointia. Niissä hyväksikäytetään vastaanottajien mahdollista hyväntahtoisuutta ja johdateltavuutta hyväksi, lähetetään huijaus valtavalle joukolle ihmisiä, jolloin todennäköisyys siitä, että jotkut menevät lankaan, kasvaa. [Sutcliffe 2019.]

Yritysten tietojen käyttöoikeusjärjestelyt kannattaa pitää selkeinä. Työntekijöille ja yhteistyökumppaneille sallitaan pääsy vain niihin tietoihin, joita he todella tarvitsevat. Sekä ylläpidetään listaa mitkä oikeudet kenelläkin on, jotta vahingon sattuessa sen suuruus voidaan selvittää. Tyytymättömät yhteistyökumppanit ja tietämättömät tai vahingolliset työntekijät saattavat kopioida, muuttaa tai jopa varastaa informaatiota. [Sutcliffe 2019.]

Täytyy myös muistaa, että virheitä tapahtuu. Järjestelmän ja työntekijöiden virheiden korjaamiseen kannattaa varautua osaavalla tietoturva-ammattilaisella. Näihin virheisiin voidaan varautua ennaltaehkäisemällä niiden mahdollisuutta, ja virheen tapahtuessa niiden vaikutukset voidaan minimoida ja välttyä suuremmilta tietovuodoilta. [Sutcliffe 2019.]

4 Yritysten käyttäjätietojen suojelu

Nykypäivänä informaation arvo on kasvamassa jopa aikaa ja rahaa korkeammaksi, koska tärkeä tieto voi säästää paljon aikaa ja tuottaa liikevoittoa. Yrityksellä on vastuu suojella asiakkaidensa ja työntekijöidensä yksityisyyttä, pitämällä heidän henkilökohtaiset tietonsa turvattuna. Yritysten täytyy ennakoida ja valmistautua mahdollisiin tietomurtoihin, ja sellaisen tapahtuessa täytyy ryhtyä vastatoimiin ja toipua murrosta. Tässä luvussa selvitetään miten yritys voi suojella järjestelmiään ja hallussa pitämiään tietoja.

4.1 Tietoverkon suojelu

Yrityksen kannattaa todentaa työntekijöiden kirjautuminen verkkoon esimerkiksi *kaksivaiheisella tunnistautumisella* (Two factor authentication), josta kerrotaan tarkemmin kappaleessa 5. Työntekijöille kannattaa sallia pääsy vain niihin tietoihin, joita he todella tarvitsevat, sekä ylläpitää listaa mitkä oikeudet kenelläkin on. Tietoverkkoon tunkeutumista täytyy ennaltaehkäistä ja havaita käyttämällä *IPS* (Intrusion Prevention System) sekä *IDS* (Intrusion Detection System) järjestelmiä, jakamalla tietoverkko osiin jotta tietomurron sattuessa koko verkko ei vaarannu kerralla, käyttämällä *hunajapurkki* (Honeypot) ansoja jotka vaikuttavat huonosti suojatuilta palvelimilta, mutta keräävätkin tietoa hyökkääjistä ja haittaohjelmista, ja pitämällä palomuuri päivitettynä ajan tasalle. [Solic *et al.* 2017.]

Tietoverkon laitteistoa täytyy valvoa säännöllisesti ja ylläpitää lokeja järjestelmän tapahtumista. Tietoverkon hallintaan kuuluu tietoliikenteen erottelu, *SNMP:n* (Simple Network Management Protocol) käyttö ja laitteiston varmuuskopioinnin ylläpito. Yrityksen langattoman verkon käyttöä tulee myös valvoa ja suojata. Verkossa käytetään yrityksen määrittämää *SSID*:tä (Service Set Identifier) jolla kytkeydytään haluttuun verkkoon. Verkon tietoturvan suojaamiseksi tulee käyttää luotettavaa tunnistamis- ja salausjärjestelmää, kuten WPA2-tietoturvastandardia ja *AES* (Advanced Encryption Standard) salausalgoritmia. Verkkoistunnoille kannattaa asettaa aikakatkaisu, ja vierailijoille tulee olla oma verkkonsa. [Solic *et al.* 2017.]

4.2 Tietokoneohjelmistojen suojelu

Ohjelmistot täytyy suojata laadukkaalla ja säännöllisesti päivitettävällä virustentorjuntaohjelmistolla, joka hoitaa tietokoneen kunnossapitoa. Koneet pitää myös turvata roskapostisuodattimella ja vakoiluohjelmilta. Sekä niiden välinen kommunikaatio, arkistot, sisältämät tiedostot ja käsiksi päästävissä olevat tiedostot, täytyy salata. [Solic *et al.* 2017.]

4.3 Varmuuskopiointi

Varmuuskopiointia varten täytyy olla määritellyt toimintaohjeet. Varmuuskopiot täytyy tehdä säännöllisesti, kopioita kannattaa säilyttää useammassa paikassa, tiedostojen päällekkäisyyttä kannattaa välttää ja varmuuskopioihin käsiksi pääsyä täytyy valvoa. [Solic *et al.* 2017.]

4.4 Turvallisuusmenetelmät

Yrityksellä täytyy olla datakäytäntöjä koskevat linjaukset. Datan käsittelyyn, analysointiin ja poistamiseen sovitut säännöt. Datavuotoja vastaan täytyy olla suoja ja henkilökohtainen data täytyy säilyttää salausmenetelmän suojissa. Lisäksi näiden linjauksien noudattamista täytyy valvoa, jotta tiedot pysyvät turvassa. [Solic *et al.* 2017.]

Tiukat salasanakäytännöt lisäävät yrityksen turvallisuutta, koska heikot salasanat ovat suurimpia uhkia tietoturvalle. Käytettävien salasanojen tulee olla tarpeeksi laadukkaita ja monimutkaisia, eikä samaa salasanaa kuulu käyttää muissa järjestelmissä. On myös tärkeää valvoa että käytäntöjä noudatetaan. [Solic *et al.* 2017.]

Yrityksen pitää varautua mahdollisiin onnettomuuksiin, ja laatia niitä varten toimintamalli. Toimintamallissa täytyy huomioida varmuuskopioiden palauttaminen, välikohtauksen hallinta, asiantuntijoille ilmoittaminen, määritellyt toimintasäännöt ja yhteydenottoihin vaaditut tiedot. [Solic *et al.* 2017.]

Työntekijöillä on myös omat velvollisuutensa turvallisuuden takaamiseksi. Kuten työsopimuksessa määritellyt seikat, yrityksen järjestämät säännölliset koulutukset ja niistä saatujen oppien hyödyntäminen ja työsuhteen päättymisen toimintaohjeet. Työntekijöitä kannattaa ohjeistaa etukäteen virheiden ja epäkohtien ilmoittamista, tietoverkon etäkäyttöä sekä verkossa käytettäviä mobiililaitteita varten. Työpaikalla on myös suotavaa toteuttaa *siistin pöydän politiikkaa* (Clean Desk Policy) ja *tyhjän näytön politiikkaa* (Clean Screen Policy). Eli työpäivän päättyessä työpiste tulee siivota, eikä esille saa jättää töihin liittyvää materiaalia, joka voisi päätyä vääriin käsiin, ja työpisteeltä hetkellisesti poistuttaessa tietokone lukitaan ja pidempien taukojen ajaksi koneelta kirjaudutaan ulos, tällöin ulkopuoliset eivät pääse käsiksi heille kuulumattomiin tietoihin. [Solic *et al.* 2017.]

4.5 Fyysinen turvallisuus

Fyysinen turvallisuus sisältää työpaikalla tapahtuvan toiminnan turvaamisen. Työntekijöiden ja ulkopuolisten henkilöiden, kuten asiakkaiden ja yhteistyökumppanien, kulkuoikeuksia kannattaa valvoa, ketkä pääsevät käsiksi tiedostopalvelimiin, henkilökohtaisiin tietokoneisiin ja tietoverkkoon. Kaapeliverkko on myös hyvä turvata. Videovalvonnalla ja videomateriaalin arkistoinnilla voi hoitaa työpaikan tarkkailun yöaikaan. Fyysiseen turvallisuuteen liittyy myös ulkoisilta uhilta, kuten tulipaloilta ja ryöstöiltä suojautuminen.

Vanhentuneiden arkistojen ja työvälineiden, niin paperisten kuin elektronistenkin, hävittäminen täytyy hoitaa turvallisesti, jotta yrityksen käsittelemää tietoa ei joudu vääriin käsiin. [Solic *et al.* 2017.]

4.6 Tietoturvaan liittyvien lakisääteisten määräysten noudattaminen

Yritysten täytyy noudattaa valtion laissa määriteltyjä suojaustasoja ja turvallisuusvaatimuksia. Ja Euroopan unionin asukkaiden käyttäjätietoja täytyy käsitellä EU:n määräysten mukaisesti. Vastuu tietoturvavelvoitteiden valvomisesta on maiden *kansallisilla turvallisuusviranomaisilla* (National Security Authority). Suomessa kansallisena turvallisuusviranomaisena toimii ulkoministeriö, ja määrättynä turvallisuusviranomaisena ja *kansallisena tietoturvaviranomaisena* (National Communications Security Authority) toimii Kyberturvallisuuskeskus. [Kyberturvallisuuskeskus 2019a.]

4.7 Verkkosivujen turvallisuus

Laitteiston kannalta tulee ottaa huomioon varmuuskopioiden olemassaolo ja tarvittaessa varaserverin toiminta, jotta sivusto pysyy käytettävissä. Myös verkkosivuja ylläpitävä laitteisto ja niiden tallentama data täytyy olla turvattuna aiemmin mainittujen menetelmien mukaan. [Solic *et al.* 2017.]

Ohjelmiston turvallisuus määräytyy osin jo ohjelmointivaiheessa, ammattimaisen ohjelmoijan koodin laatu on korkealla, tällöin ohjelma sisältää todennäköisesti vähemmän tietoturvariskejä. Ohjelmistopuolella täytyy ottaa huomioon etäkäyttö ja ylläpito, tietoliikenne täytyy salata esimerkiksi *TLS* (Transport Layer Security) salausprotokollalla. Sivustoa pitää ylläpitää säännöllisesti ja komponenttien päivitykset täytyy olla ajan tasalla tietomurtoriskin minimoimiseksi. Käyttäjiltä kannattaa vaatia mahdollisimman monimutkaisia salasanoja ja mieluusti mahdollistaa kaksivaiheinen tunnistautuminen. [Solic *et al.* 2017.]

5 Tunnistautuminen järjestelmissä

Monet järjestelmät luottavat edelleen staattisiin salasanoihin käyttäjien identifioimisessa. Pelkkien salasanojen käyttöön liittyy kuitenkin merkittäviä tietoturvaongelmia. Käyttäjillä on tapana käyttää helposti arvattavissa olevia salasanoja, käyttää samaa salasanaa useassa järjestelmässä ja pitää salasanoja muistissa laitteillaan. Tällöin hakkereilla on monia eri keinoja päästä heille kuulumattomiin salasanoihin käsiksi. On olemassa keinoja, jotka vahvistavat salasanojen käyttöä, kuten uusien salasanojen vaihtaminen tarpeeksi usein ja tarpeeksi monimutkaisten salasanojen käyttäminen, mutta peruskäyttäjät noudattavat näitä keinoja aivan liian harvoin. [Aloul *et al.* 2009.]

Kaksivaiheinen tunnistautuminen on kehitetty yritysten tarpeisiin tarjota vahvempia tunnistautumismenetelmiä asiakkailleen ja työntekijöilleen [Aloul *et al.* 2009]. Kaksivaiheinen tunnistautuminen voi perustua teknisesti eri menetelmiin. Yhteistä menetelmille on se, että niissä käytetään vähintään kahta seuraavista todentamistekijöistä [Kyberturvallisuuskeskus 2019b]:

- Tiedossa oloon perustuva todentamistekijä, jonka henkilön on osoitettava olevan tiedossaan. Esimerkiksi salasana tai PIN-koodi.
- Hallussapitoon perustuva todentamistekijä, jonka henkilön on osoitettava olevan hallussaan. Esimerkiksi tunnuslukulaite, mobiilisovellus, tekstiviestivarmennus tai tunnuslukulista.
- Luontainen todentamistekijä, joka perustuu johonkin henkilön fyysiseen ominaisuuteen. Esimerkiksi sormenjälki tai iiris.

Kahden todentamistekijän käyttäminen on huomattavasti vahvempi ja turvallisempi tapa suojata käyttäjän tiedot kuin perinteinen yhden todentamistekijän menetelmä. Esimerkiksi rahan nostaminen pankkiautomaatilta hyödyntää kahden todentamistekijän menetelmää. Käyttäjällä pitää olla hallussaan pankkikortti, joka toimii hallussapitoon perustuvana todentamistekijänä, sekä käyttäjän pitää tietää PIN-koodi, joka on tiedossa oloon perustuva todentamistekijä. [Aloul *et al.* 2009.]

Koska lähes jokainen omistaa nykyään kännykän, edullisin ja käyttäjälle helpoin keino on mobiilisovellus, jolla kaksivaiheinen tunnistautuminen tapahtuu. Tällöin ei tarvitse maksaa esimerkiksi varmistustekstiviestin lähettämisestä tai tunnuslukulistan materiaaleista, valmistamisesta ja toimittamisesta, eikä ole kovin suurta riskiä siitä että kyseinen varmennuskeino pääsisi katoamaan [Aloul *et al.* 2009].

Biometriikat kuten sormenjälki ja iiris ovat huomattavasti turvallisempia todentamismenetelmiä, mutta niitä ei vielä juurikaan käytetä verkossa tai pankkiautomaateilla, laitteiston kalliin hinnan vuoksi. [Aloul *et al.* 2009.] Puhelinvalmistajat ovat alkaneet hyödyn-

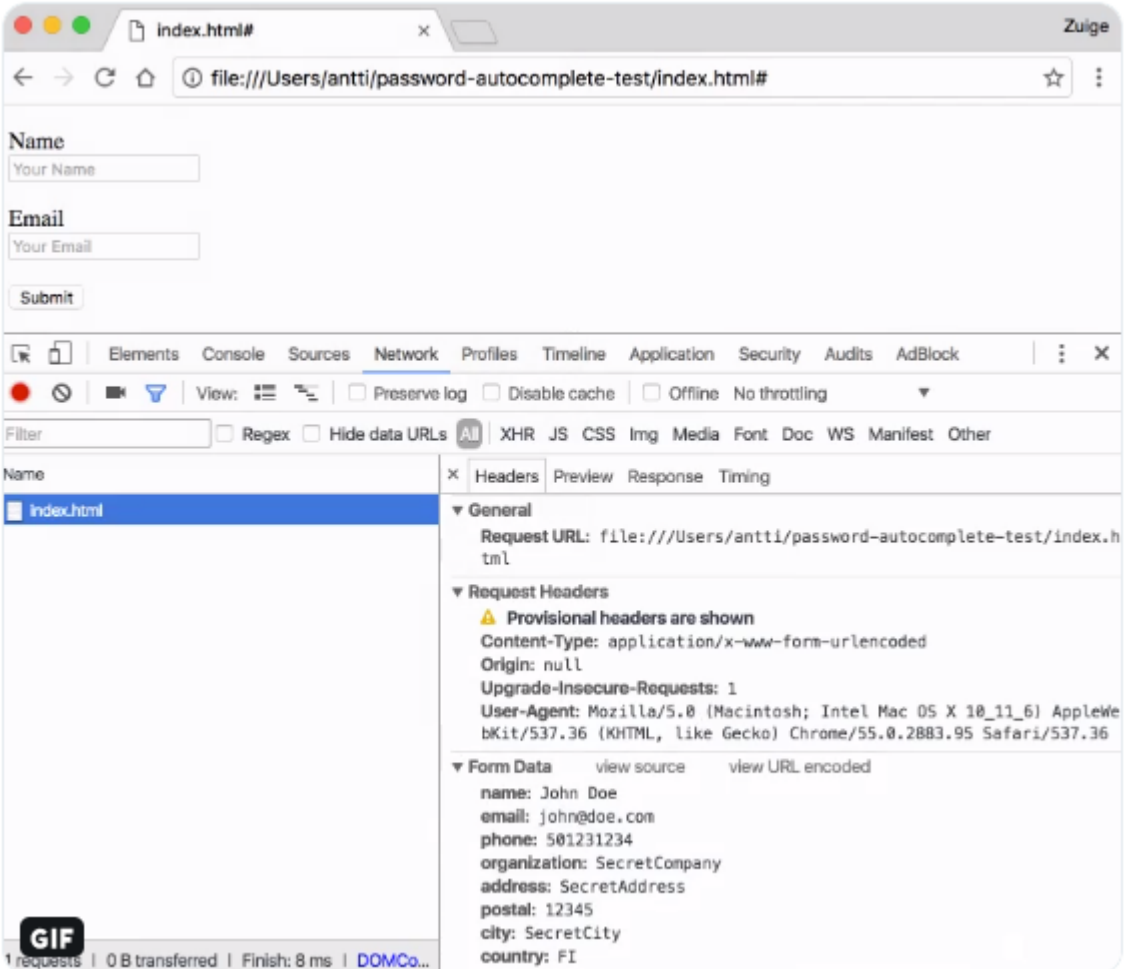
tämään biometriikan käyttöä lukitusjärjestelmissään. Sormenjälkilukija on jo täysin arkipäivää matkapuhelimissa, mutta niiden turvallisuus on vielä hieman kyseenalaista. Applen kehuessa Touch ID -järjestelmänsä loistavaa turvallisuutta, järjestelmä on hakkeroitu muovailuvahan avulla. Hakkeri käytti hammastahnavalosta sormenjäljestä luodakseen siitä kopion muovailuvahalla, ja sai avattua iPhone 6 lukituksen tämän muovailuvahasormenjäljen avulla. [Muhammad 2018.]

New Yorkin yliopistossa ja Michiganin osavaltion yliopistossa on onnistuttu luomaan *yleissormenjälkiä* (Master fingerprint), joilla pystyy huijaamaan sormenjälkilukijoita jopa 65% todennäköisyydellä. Yleissormenjäljet on luotu käyttämällä oikeissa sormenjäljissä toistuvia kaavoja. Älypuhelinten sormenjälkilukijat ovat suhteellisen pieniä, ja skannaavat kerralla vain osia sormenjäljistä. Yleissormenjäljet toimivat koska on paljon todennäköisempää löytää sopiva osa sormenjäljestä, jolla huijata sormenjälkilukijaa, kokonaisen sormenjäljen sijaan. [Titcomb 2017.]

6 Käyttäjä: näin pidät tietosi turvassa

Myös peruskäyttäjä voi vaikuttaa henkilökohtaisten tietojensa turvallisuuteen. Omia tietojaan kannattaa luovuttaa vain luotettaville tahoille, ja heillekin vain tiedoista välttämättömimmät. Uniikkien ja mahdollisimman monipuolisten salasanojen käyttö parantaa käyttäjätilien turvallisuutta, eikä salasanoja saa säilyttää laitteillaan muistissa salaamattomissa tiedostoissa. Kaksivaiheista tunnistautumista kannattaa käyttää aina kun se on mahdollista. Pidä tietokoneesi ajan tasalla, päivitysten myötä parannetaan sovellusten tietoturvaa ja korjataan ilmenneitä heikkouksia, joten kannattaa aina päivittää käyttöjärjestelmä, sovellukset ja virusturva uusimpiin versioihin. [Pitkänen 2014.]

Eri palveluihin kirjautumista kannattaa harkita. On olemassa selaimen vuotamia tietoja analysoiva sivusto [Privacy 2019] joka havaitsee, että esimerkiksi minun koneellani on kirjauduttuna sisään palveluihin: Gmail, Youtube, Slack ja Spotify. Kyseinen sivusto saa myös selville mitä selainversiota ja käyttöjärjestelmää käytän, ja mille kielelle sekä aikavyöhykkeelle koneeni on asetettu. Nämä tiedot ovat siis kaikkien sivustojen saatavilla käyttäjän tietämättä.



Kuva 4. Kehittäjän työkalusta näkyy että sivusto sisältää piilotettuja tekstikenttiä [Kuosmanen 2017].

Automaattista lomakkeiden täyttöä kannattaa välttää. Viljami Kuosmanen huomasi, että verkkosivuilla saattaa olla käyttäjältä piilotettuja tekstikenttiä, jotka keräävät huomaamatta tietoja käytettäessä automaattista lomakkeiden täyttöä. Kuvassa 4 sivusto kysyy näennäisesti vain käyttäjän nimeä ja sähköpostiosoitetta, mutta kehittäjän työkalulla havaitaan, että sivusto saa automaattista täydennystä käytettäessä haltuunsa myös käyttäjän puhelinnumeron, organisaation, katuosoitteen, postinumeron, kaupungin sekä valtion. [Kuosmanen 2017.]

Julkisten *WLAN*-verkkojen (Wireless Local Area Network) käyttämistä kannattaa varoa, neuvoo F-Securen toimitusjohtaja Mikko Hyppönen [Pitkänen 2014]. Ne ovat käteviä langattomia lähiverkkoja esimerkiksi kahviloissa, mutta ne ovat suojaamattomia ja kuka tahansa voi seurata verkossa tapahtuvaa liikennettä. Varsinkin yksityisimpien tietojen siirtämistä kyseisissä verkoissa ilman suojausta kannattaa välttää. [Pitkänen 2014]

Yleistyneet pilvipalvelut ovat kätevä tapa turvata tiedostojen säilyvyys. Ne eivät kuitenkaan sovellu ainakaan kaikista yksityisimmille tiedoille, kuten salasanalistoille, kertoo tietoturva-asiantuntija Aleksi Tarhonen Viestintävirastosta [Pitkänen 2014]. Kannattaa myös torjua ja poistaa verkkosivujen evästeet säännöllisesti, niiden avulla seurataan käyttäjän internetin selailua. Sosiaalisten medioiden yksityisyysasetukset kannattaa käydä tarkasti läpi, jotta yksityisimmät, esimerkiksi lomareissusta, jakamasi tiedot eivät leviä turhan laajalle ja aiheuta hankaluuksia. [Pitkänen 2014.]

On suositeltavaa vältellä epäilyttäviä sivustoja ja sähköpostiviestejä. Ne voivat sisältää haittaohjelmia ja pyrkiä kalastelemaan käyttäjiltä tietoja. Kyseenalaisten liitteiden tai linkkien avaaminen saattaa avata hakkerille väylän päästä käsiksi laitteeseen ja sen tiedostoihin.

7 Yhteenveto

Tutkielmasta käy ilmi, että käyttäjätietojen suojelu on täysin aiheellista ja haastavaa toimintaa. Vaikka yritykset luulevat tekevänsä tarpeeksi tietojensa suojeluun, tietomurtoja tapahtuu valtavasti. Euroopan unionin määräämä asetus oli todellakin ajankohtainen ja paransi selkeästi käyttäjien oikeuksia ja yritysten velvollisuuksia käyttäjätietojen suhteen. Käyttäjät voivat tehdä parhaansa tietojensa turvallisuuden maksimoimiseksi, mutta joutuvat lopulta luottamaan, että yritys tekee oman osansa moitteetta, toki käyttäjä voi mahdollisuuksien mukaan päättää minkä yrityksen asiakkaaksi ryhtyy. Henkilötietojen salassapito vaatii vaivannäköä monelta eri taholta, mutta jos kaikki tekevät parhaansa, tietojen salassa pysyminen on mahdollista.

Jäädään innolla odottamaan EU:n seuraavaa tietosuojaan liittyvää asetusta, mahtaakohan siihen vierähtää taas 20 vuotta. Seurataan hakkerien toimintaa ja uusien heikkouksien etsimistä järjestelmistä. Tarkkaillaan yritysten keinoja välttyä tietomurroilta, sekä kehittää entistä parempia turvallisuus- ja salausjärjestelmiä. Ja pysytään organisaatioiden asiakkaina ja järjestelmien käyttäjinä, tehden parhaamme tietojemme varjelemiseksi.

8 Viiteluettelo

Aïmeur, Esma & Manuel Lafond. 2013. The scourge of internet personal data collection. In: *2013 International Conference on Availability, Reliability and Security.*

Aloul, Fadi; Syed Zahidi & Wassim El-Hajj. 2009. Two factor authentication using mobile phones. In: *2009 IEEE/ACS International Conference on Computer Systems and Applications.*

Armerding, Taylor. 2018. The 18 biggest data breaches of the 21st century. CSO.

Business Insider. 2018. This is why your inbox is suddenly full of notices about privacy policies. https://www.businessinsider.co.za/gdpr-notices-are-filling-email-inboxes-because-it-comes-into-effect-today-2018-5 Checked 15.8.2019

EU gdpr.org. 2019. GDPR FAQs. https://eugdpr.org/the-regulation/gdpr-faqs/ Checked 13.8.2019

Facebook. 2019. Tietosi. https://www.facebook.com/settings?tab=your_facebook_information Haettu 17.8.2019

Joseph, Rhoda C. 2017. Data breaches: Public sector perspectives. IT Professional. Volume 20. Issue 4. 57-64.

Kuosmanen, Viljami. 2017. This is why I don't like autofill in web forms. https://twitter.com/anttiviljami/status/816585860661518336 Checked 18.8.2019

Kyberturvallisuuskeskus. 2019a. NCSA. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa Haettu 18.8.2019

Kyberturvallisuuskeskus. 2019b. Sähköinen tunnistaminen. https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen Haettu 12.8.2019

Macaulay, Tom. 2019. The biggest ICO fines for data protection breaches and GDPR contraventions. Computerworld.

Meszaros, Janos. 2018. The conflict between privacy and scientific research in the GDPR. In: *2018 Pacific Neighborhood Consortium Annual Conference and Joint Meetings (PNC).*

Muhammad, Nooh Bany. 2018. A study on cell phone security: Authentication techniques. In: *2018 International Conference on Information and Computer Technologies (ICICT).*

O'Flaherty, Kate. 2019. Marriott CEO reveals new details about mega breach. Forbes.

Pitkänen, Perttu. 2014. Kymmenen vinkkiä: Näin suojaat yksityisyyttäsi netissä. Ilta-Sanomat.

Porter, Jon. 2019. Google fined €50 million for GDPR violation in France. The Verge.

Privacy. 2019. Privacy Analyzer. https://privacy.net/analyzer/ Checked 18.8.2019

Privazyplan. 2019. Recital 33. http://www.privacy-regulation.eu/fi/r33.htm Checked 13.8.2019

Solic, K., H. Ocevcic, I. Fosic, I. Horvat, M. Vukovic & T. Ramljak. 2017. Towards overall information security and privacy taxonomy. In: *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).*

Suomisanakirja. 2019. Tietovuoto. https://www.suomisanakirja.fi/tietovuoto Haettu 18.8.2019

Sutcliffe. 2019. The 8 most common causes of data breach. https://www.sutcliffe-insurance.co.uk/news/8-most-common-causes-of-data-breach/ Checked 17.8.2019

Tietosuojavaltuutetun toimisto. 2019. Usein kysyttyä EU:n tietosuoja-asetuksesta. https://tietosuoja.fi/gdpr Haettu 13.8.2019

Titcomb, James. 2017. Why your smartphone's fingerprint scanner isn't as secure as you might think. The Telegraph.

Valtiovarainministeriö. 2016. Lainsäädännön taustaa. https://www.vah-tiohje.fi/web/guest/lainsaadannon-taustaa Haettu 18.8.2019

Zou, Hui. 2016. Protection of personal information security in the age of Big Data. In: *2016 12th International Conference on Computational Intelligence and Security (CIS)*.